

Marcel Rémon

`marcel.remon@fundp.ac.be`

Département de Mathématique,
Facultés Universitaires Notre-Dame de la Paix, B-5000 Namur, Belgique



VISIT...

LANZAROTE
Caliente.COM

Plan du cours

- ① Les racines : la logique des anciens d'Aristote aux stoïciens
- ② Le vocabulaire et le formalisme : langage, modèle, structure, cohérence, complétude, ...
- ③ La logique des prédicats du premier ordre.
- ④ La théorie des ensembles et la construction des nombres

Plan du cours (suite)

- ⑤ La question de l'infini : les idées géniales et dangereuses de Cantor (les classes cardinales et les $\aleph$)
- ⑥ L'auto-référence et les théorèmes de Gödel.
- ⑦ Conclusions et discussion.

La syntaxe de la logique formelle

“Le nom de la chanson s’appelle *Les yeux de morue*”

“Ah ! C’est donc cela le nom de la chanson”, dit Alice essayant de paraître intéressée.

“Non, vous ne comprenez pas”, reprit le cavalier un peu contrarié, c’est ainsi qu’on appelle ce nom. Son véritable nom est *Le très très vieil homme*.”

“J’aurais dû dire : c’est ainsi que s’appelle la chanson”, dit Alice pour se corriger.

“Sûrement pas, c’est tout autre chose, la chanson s’appelle *Voies et moyens*, mais c’est seulement ainsi qu’elle s’appelle, vous voyez ?”

“Mais alors, la chanson, qu’est-ce que c’est ?” s’écrie Alice, complètement éberluée.

“J’allais le dire”, répond le cavalier, “la chanson elle-même est *Assis sur la barrière* et l’air est de mon invention.

Lewis Carroll, *De l’autre côté du miroir*

Syntaxe : le langage

① Définitions :

- **Les signes** : Ce sont une série d'objets appartenant à une liste finie ou tels qu'un procédé permette de reconnaître cet objet comme un signe dans un temps fini (*effectivité de la définition d'un signe*)
- **Les termes** : Il s'agit d'assemblages de signes à partir de *règles effectives*.
- **Les formules** : Il s'agit d'assemblages de termes et de signes à partir de *règles effectives*.

Syntaxe : le langage

② **Exemple** : Le langage PE

(Hofstadter D., Gödel, Escher, Bach : Les brins d'une Guirlande Eternelle, Paris, 1985)

- **Les signes** : ' P ', ' E ' et la barre '|'
- **Les termes** : N'importe quelle suite non vide de barres '|'. Par exemple, '|||', '|'| ou '|||||'.
- **Les formules** : Il s'agit d'un premier terme suivi du signe ' P ', puis d'un autre terme, puis de ' E ' et d'un troisième terme.
Par exemple : '|||| P || E ||||'

Syntaxe : le langage

③ Exemple : Le langage BARON

- **Les signes** : la barre '|', le rond '○' et le trait '—'
- **Les termes** : le mot formé du seul '○' ou une suite de '|' et de '○' commençant par une '|'.
Par exemple, '○', '|○' ou '|| ○ ||○'.
- **Les formules** : Il s'agit d'une suite alternée de traits '—' et de termes qui commencent et finissent par un trait. Par exemple : '— | ○ — || ○ || —'

Terminologie : On dit que le terme T est *plus simple que* S s'il a moins de signes ou s'ils en ont le même nombre mais que le premier signe différent dans T et dans S est un rond dans T . Si F et G sont des formules, on dit que F est un *prédécesseur* de G si F a les mêmes termes que G sauf un qui est plus simple.

Syntaxe : la langue

① Définitions :

- **La langue** : la langue formelle est un langage formel muni de règles d'inférence effectives qui permettent de déduire une formule appelée **conclusion** d'un ensemble de formules appelées **prémisses**.
- **Les règles d'inférence** : Ce sont les règles qui permettent cette déduction. Leur *caractère effectif* signifie qu'il doit être possible de déterminer en un temps fini si un ensemble de formules peut servir de prémisses et si une formule donnée en est la conclusion.

Syntaxe : la langue

② Exemple : la langue PE

- Règle d'inférence unique :
Si x, y et z désignent des suites non vides de barres, de la formule $xPyEz$ comme prémisse, on peut déduire $xPy|Ez|$ comme conclusion.

③ Exemple : la langue BARON

- Règle d'inférence unique :
D'un ensemble $\mathcal{E}$ de formules prises comme prémisses, on peut déduire une formule F si tout prédécesseur de F a un prédécesseur dans $\mathcal{E}$

Syntaxe : la théorie

① Définitions :

- **La théorie** : la théorie est une langue munie de règles effectives qui déterminent un ensemble de formules appelées **axiomes**.
- **Les démonstrations** : Ce sont des suites finies de formules telle que chacune d'elles soit un axiome ou une conclusion d'un ensemble de prémisses qui la précèdent.
- **Les théorèmes** : Ce sont des formules figurant dans une démonstration. On note que F est un théorème dans la théorie $\mathcal{T}_h$ par $\mathcal{T}_h \vdash F$

Syntaxe : la théorie

① Définitions :

- Une théorie est dite **décidable** s'il existe pour toute formule de la langue un procédé effectif pour décider si cette formule est un théorème ou non.
- On désigne par $(\mathcal{T}_h, F)$ la théorie obtenue en ajoutant la formule F aux axiomes de la théorie $\mathcal{T}_h$.

② Exemple : la théorie PE

- **Axiomes** : Si x est une suite non vide de barres, ' $xP|Ex|$ ' est un axiome.
- **Exemples de théorèmes** : ' $||P|E|||$ ', ' $||P||E|||$ '.

Syntaxe : la théorie

③ Exemple : la théorie BARON

● **Axiomes** : Ce sont les formules sans barre.

● **Exemples de démonstration** :

(a) — ○ — ○ — ○ — ○ —

(b) — | — ○ — | — ○ —

(c) — ○ — ○ — | — | —

(d) — | ○ — ○ — | ○ — ○ —

● **Remarques** : La première formule est un axiome. La deuxième a comme prédécesseurs — ○ — ○ — | — ○ — et — | — ○ — ○ — ○ — qui ont l'axiome — ○ — ○ — ○ — ○ — comme prédécesseur.

La sémantique de la logique formelle

- ◇ “Une illusion peut-elle exister ?” ◇ “Quel est le bruit d’une seule main qui applaudit ?”
- ◇ “Lorsqu’il n’y a plus rien à faire, que faites-vous ?”
- ◇ “Qu’y a-t-il au-delà de l’espace infini ?” ◇ “La vague et la mer ne font qu’un.”
- ◇ “Shuzan montra son kyôsku aux moines, et dit : Si vous appelez cela un petit bâton, vous n’exprimez pas la réalité. Si vous ne l’appelez pas un petit bâton, vous niez sa nature. Alors ... comment appelez-vous ceci ?”
- ◇ “Lorsqu’on posait une question au maître Gutei, il montrait son doigt. Un jour, lorsque le maître posa une question, un élève décida de l’imiter. Gutei lui coupa le doigt ! Celui-ci hurla de douleur et s’enfuit en courant. Gutei le rappela. Lorsque l’élève se retourna, Gutei leva son propre doigt ... et soudain son élève réalisa l’éveil.”

Koans Zen

Le domaine d'interprétation

① Définitions :

- Un domaine d'interprétation est formé d'un domaine $\mathcal{D}$ ou ensemble non vide d'éléments appelés **objets** et d'un ensemble de règles permettant d'associer à chaque formule F une phrase $F_{\mathcal{D}}$ relative à certains objets et susceptible d'être **vraie ou fausse**.
- Cette notion de vérité doit répondre à **la logique classique**. Elle doit vérifier **le principe du tiers exclu** et **le principe de la double négation**.
- Notation : $\mathcal{D} \models F$ signifie que l'interprétation de F dans $\mathcal{D}$ est vraie ou $F_{\mathcal{D}}$ est vraie.

Sémantique : l'interprétation

② Exemple : Le langage PE

- L'interprétation **PRODUIT-ÉGAL** : Soit une formule F composée de trois suites comprenant x , y et z barres séparées par un ' P ' et puis par un ' E ' :

$$\overbrace{\text{||||}}^x P \overbrace{\text{||||}}^y E \overbrace{\text{|||||}}^z$$

On lui associe la phrase F_D : *le produit de x par y est égal à z .*

- L'interprétation **PLUS-ÉGALE** : On associe à F la phrase F_D : *la somme de x par y est égale à z .*

Sémantique : l'interprétation

③ Exemple : Le langage BARON

- **L'interprétation des termes** : A tout terme T , nous associons le polynôme P_T dont la suite des coefficients est obtenue en remplaçant dans le terme T une barre par le chiffre 1 et un rond par le chiffre 0. Par exemple, le terme ' $|| \bigcirc |$ ' correspond au polynôme $X^3 + X^2 + 1$.
- **L'interprétation des formules** : A une formule F , on associe la phrase : $F_{\mathbb{Z}/2\mathbb{Z}} \stackrel{\text{def}}{\iff}$ *la somme des polynômes associés aux termes de F est nulle dans $\mathbb{Z}/2\mathbb{Z}$.*

Les Structures et Modèles

① Définitions :

- Une structure pour une langue est un domaine d'interprétation compatible avec les règles d'inférence. *Si des prémisses sont interprétées par des phrases vraies, leur conclusion l'est aussi.*
- Un modèle d'une théorie est une structure compatible avec les axiomes, c'est-à-dire que les axiomes soient interprétés par des phrases vraies. Par conséquent, dans un modèle, tous les théorèmes sont interprétés par des phrases vraies.

Les Structures et Modèles

② Exemples :

- L'interprétation **PRODUIT-ÉGAL** ne conduit pas à une structure pour la langue PE.
- L'interprétation **PLUS-ÉGALE** conduit à une structure pour la langue PE.
- L'interprétation **PLUS-ÉGALE** conduit à un modèle pour la théorie PE, car x plus 1 égal $x + 1$ (axiomes).
- L'interprétation **Polynômes de $\mathbb{Z}/2\mathbb{Z}[X]$** conduit à un modèle pour la théorie BARON (exercice à faire).

Cohérence et Complétude

① Définitions :

- Une théorie est dite **cohérente, consistante ou non contradictoire** si toutes les formules ne sont pas des théorèmes. **Conséquence** : Une théorie qui a un modèle où certaines formules s'interprètent par des phrases fausses est cohérente.
- Une théorie est dite **complète par rapport à un modèle** si toutes les formules qui se traduisent par une phrase vraie sont des théorèmes.
- Une théorie est **décidable** si on peut décider en un temps fini qu'une phrase est vraie ou fausse.

Cohérence et Complétude

② Exemples :

- La théorie PE est complète par rapport au modèle PLUS-ÉGALE. En effet, si F s'interprète par une phrase vraie $x + y = z$, on peut démontrer que F est un théorème.
- La théorie PE est cohérente. En effet, il existe des formules qui ne sont pas des théorèmes : $|||P|E|||$.
- La théorie BARON est cohérente : $\neg \mid \neg$ s'interprète comme une phrase fausse dans $\mathbb{Z}/2\mathbb{Z}[X]$.
- La théorie BARON est complète par rapport au modèle des polynômes.

La logique des propositions

① Syntaxe : Le langage PRÉDICATS

● Les **signes** sont :

- (a) Les lettres $v^1, v^2, \dots, v^n$, appelées aussi variables.
- (b) Les symboles prédicatifs ou prédicats (du premier ordre), notés Ψ_i^j . Le nombre i désigne le nombre de place du prédicat, le nombre j étant le numéro du symbole. Le signe Ψ_2 ou Ψ_2^0 se désigne par "=".
- (c) Les symboles fonctionnels notés Φ_i^j .
- (d) Les symboles logiques : ' $\wedge$ ', ' $\neg$ ' et ' $\forall$ '.

La logique des propositions

② Syntaxe : Le langage PRÉDICATS

- Les **termes bien formés** sont : les lettres et les symboles fonctionnels à n places suivi de n termes déjà construits.
- **Exemples** : $v^2, \Phi_0^2, \Phi_3^2 v^2 \Phi_0^2 v^2$.
- **Les formules** sont :
 - (a) Un symbole prédictatif à n places suivi de n termes (formule **atomique**).
 - (b) $\wedge$ suivi de deux formules déjà construites.
 - (c) $\neg$ suivi d'une formule déjà construite.
 - (d) $\forall$ suivi d'une variable puis d'une formule.

La logique des propositions

③ Syntaxe : Le langage PRÉDICATS

● **Notations :** (F et G formules, x variable)

● $(F \wedge G) \stackrel{\text{def}}{\iff} \wedge FG$

● $(F \vee G) \stackrel{\text{def}}{\iff} \neg(\neg F \wedge \neg G)$

● $(F \Rightarrow G) \stackrel{\text{def}}{\iff} \neg(F \wedge \neg G)$

● $(F \Leftrightarrow G) \stackrel{\text{def}}{\iff} ((F \Rightarrow G) \wedge (G \Rightarrow F))$

● $\exists x F \stackrel{\text{def}}{\iff} \neg \forall x \neg F$

● $!x F \stackrel{\text{def}}{\iff} \forall x \forall y ((F \langle x \rangle \wedge F \langle y \rangle) \Rightarrow x = y)$

● $\exists !x F \stackrel{\text{def}}{\iff} (\exists x F \wedge !x F)$

● La variable x de $\forall x F \langle x, y \rangle$ est dite liée alors que y est dite libre.

La logique des propositions

④ Syntaxe : La langue PRÉDICATS

- Les deux règles d'inférence :
 - LE MODUS PONENS : Si F et G sont des formules, de F et $(F \Rightarrow G)$ comme prémisse, on peut déduire G comme conclusion.
 - LA GÉNÉRALISATION : Si x est une variable, d'une formule F comme prémisse, on peut déduire la formule $\forall x F$

● Symboliquement :

$$\frac{F \quad (F \Rightarrow G)}{G} \qquad \frac{F}{\forall x F}$$

La logique des propositions

⑤ Syntaxe : La théorie de la langue PRÉDICATS

- L'ensemble des formules de la logique des propositions :

Soit $\mathcal{B}$ un ensemble de formules composées d'un seul signe (les symboles prédicatifs à zéro place) :

$$\mathcal{B} = \{F_1, F_2, \dots, F_n, P, Q, T, \dots\}$$

Ces formules seront interprétées comme vraies ou fausses.

Soit $\mathcal{P}$ l'ensemble des formules qu'on peut former à partir de $\mathcal{B}$ et des règles du $\neg$ et du $\wedge$ = l'ensemble des formules de la logique des propositions.

La logique des propositions

⑥ Syntaxe : La théorie de la langue PRÉDICATS

- Les tables de vérité sur $\mathcal{B}$:

Table de $\neg$

P	$\neg P$
0	1
1	0

Table de $\wedge$

P	Q	$P \wedge Q$
0	0	0
0	1	0
1	0	0
1	1	1

La logique des propositions

⑦ Syntaxe : La théorie de la langue PRÉDICATS

- Les tables de vérité sur $\mathcal{B}$ se généralisent sur $\mathcal{P}$.

Exemple : $(P \Leftrightarrow Q) \stackrel{\text{def}}{\Leftrightarrow} (\neg(P \wedge \neg Q)) \wedge (\neg(Q \wedge \neg P))$

Table de $P \Leftrightarrow Q$

P	Q	$(\neg$	$(P$	$\wedge$	$\neg$	$Q))$	$\wedge$	$(\neg$	$(Q$	$\wedge$	$\neg$	$P))$
0	0	1	0	0	1	0	1	1	0	0	1	0
0	1	1	0	0	0	1	0	0	1	1	1	0
1	0	0	1	1	1	0	0	1	0	0	0	1
1	1	1	1	0	0	1	1	1	1	0	0	1

La logique des propositions

⑧ Syntaxe : La théorie de la langue PRÉDICATS

● Les Tautologies de $\mathcal{P}$:

Formules de $\mathcal{P}$ dont la table de vérité donne toujours 1. Exemple : $(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$

P	Q	$(P \Rightarrow Q)$	$\Leftrightarrow$	$(\neg Q \Rightarrow \neg P)$
0	0	1	1	1
0	1	1	1	0
1	0	0	1	1
1	1	1	1	1

La logique des propositions

⑨ Syntaxe : La théorie de la langue PRÉDICATS

- La preuve par l'absurde $[(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)]$:
Pour démontrer Q comme conclusion de P (ou d'une théorie $\mathcal{T}_h$), on suppose que Q est faux ($\neg Q$ est vrai) et on montre que cela entraîne $\neg P$ (ou que P est impossible ou absurde dans $\mathcal{T}_h$).

Ex. : Démontrer $(P \Rightarrow (Q \vee T)) \Rightarrow (\neg Q \Rightarrow (P \Rightarrow T))$

$(P$	$\Rightarrow$	$(Q \vee T))$	$\Rightarrow$	$(\neg$	Q	$\Rightarrow$	$(P$	$\Rightarrow$	$T))$
1	1	0	0	1	0	0	1	0	0
"7"	2	"6 - 8"	1	4	6	3	7	5	8

La logique des prédicats de 1^{ier} ordre

NB.: La théorie de la langue PRÉDICATS est la base de beaucoup de systèmes logiques (voir la théorie des ensemble).

Définition : La logique des prédicats de 1^{ier} ordre est la théorie de la langue PRÉDICATS dont les axiomes sont :

① Les Tautologies sur $\mathcal{P}$

② Le schéma de particularisation :

Si x est une variable, si $F \langle x \rangle$ est une formule, si T est un terme et si le remplacement de x par T dans $F \langle x \rangle$ ne crée pas de confusion, alors la formule suivante est un axiome : $\forall x F \langle x \rangle \Rightarrow F \langle T \rangle$

La logique des prédicats de 1^{er} ordre

③ Le schéma de généralisation de la conclusion :

Si x est une variable, si $F \langle x \rangle$ est une formule et si G est une formule qui ne contient pas d'occurrence libre de x , alors la formule suivante est un axiome :

$$\forall x (G \Rightarrow F \langle x \rangle) \Rightarrow (G \Rightarrow \forall x F \langle x \rangle)$$

④ La réflexivité de l'égalité : $\forall x \ x = x$

⑤ Le schéma de l'égalité :

Si x, y et z sont des variables, si $F \langle x \rangle$ est une formule et si le remplacement de x par y ou par z dans $F \langle x \rangle$ ne crée pas de confusion, alors la formule suivante est un axiome : $\forall y \ \forall z \ [y = z \Rightarrow (F \langle y \rangle \Rightarrow F \langle z \rangle)]$

La logique des prédicats de 1^{er} ordre

- Quelques exemples de démonstration de méta-théorèmes simples :

	A	(Hypothèse)
A	B	(Hypothèse)
B	<i>Dém.:</i> $A \Rightarrow (B \Rightarrow A \wedge B)$	(Tautologie)
$A \wedge B$	$B \Rightarrow A \wedge B$	(Modus Ponens)
	$A \wedge B$	(Modus Ponens)

La logique des prédicats de 1^{er} ordre

• Quelques exemples de démonstration (suite) :

$$\frac{A \Rightarrow C \quad B \Rightarrow C}{A \vee B \Rightarrow C}$$

$\Downarrow$

$$A \Rightarrow C$$

(Hypothèse)

$$B \Rightarrow C$$

(Hypothèse)

$$(A \Rightarrow C) \Rightarrow [(B \Rightarrow C) \Rightarrow (A \vee B \Rightarrow C)]$$

(Tautologie)

$$(B \Rightarrow C) \Rightarrow (A \vee B \Rightarrow C)$$

(Modus Ponens)

$$A \vee B \Rightarrow C$$

(Modus Ponens)

La logique des prédicats de 1^{er} ordre

• Quelques exemples de démonstration de syllogisme :

$F \Rightarrow G$ ("Être Liégeois $\Rightarrow$ Être Belge")

$G \Rightarrow H$ ("Être Belge $\Rightarrow$ Être Européen")

$F \Rightarrow H$ ("Être Liégeois $\Rightarrow$ Être Européen")

$\Downarrow$

$F \Rightarrow G$ (Hypothèse)

$G \Rightarrow H$ (Hypothèse)

$(F \Rightarrow G) \Rightarrow [(G \Rightarrow H) \Rightarrow (F \Rightarrow H)]$ (Tautologie)

$(G \Rightarrow H) \Rightarrow (F \Rightarrow H)$ (Modus Ponens)

$F \Rightarrow H$ (Modus Ponens)

La logique des prédicats de 1^{er} ordre

• Quelques exemples de démonstration de syllogisme :

$F \Rightarrow G$ ("Tout homme est mortel")

$F <a>$ ("Socrate est un homme")

$G <a>$ ("Socrate est mortel")



$F \Rightarrow G$ (Hypothèse)

$\forall x (F <x> \Rightarrow G <x>)$ (Généralisation)

$(F <a> \Rightarrow G <a>)$ (Particularisation)

$F <a>$ (Hypothèse)

$G <a>$ (Modus Ponens)

Les structures de 1^{ier} ordre

① L'interprétation des signes :

- Soit $\mathcal{D}$ un domaine d'interprétation non vide. Ses éléments sont appelés *objets*.
- À chaque symbole prédicatif Ψ à n places, on associe une partie $\Psi_{\mathcal{D}}$ de $\mathcal{D}^n$. Le symbole " $=$ " est associé à la diagonale $\Delta_{\mathcal{D}} = \{(a, a) : a \in \mathcal{D}\}$.
- À chaque symbole fonctionnel Φ à n places, on associe une application $\Phi_{\mathcal{D}} : \mathcal{D}^n \rightarrow \mathcal{D}$.
- À chaque constante c , on associe un objet $c_{\mathcal{D}}$ de $\mathcal{D}$.

Les structures de 1^{ier} ordre

② Exemple d'interprétation des termes et des formules :

- Soit $\mathcal{D} = \{\text{Jean, Marie, Jacques, Jules, Pierre}\}$. On suppose que Jean et Marie sont les parents de Jacques, Jules et Pierre.
- La formule atomique $\Psi_2^j v_1 v_2 \equiv "v_1 \text{ et } v_2 \text{ sont frères}"$
On associe alors à Ψ_2^j la partie : $\{(\text{Jacques, Jules}), (\text{Jacques, Pierre}), (\text{Jules, Pierre})\} = \Psi_2^j \mathcal{D} \in \mathcal{D}^2$.
- La formule $\Psi_2^k v_1 v_2 \equiv "v_1 = v_2" \Rightarrow \Psi_2^k \mathcal{D} = \Delta_{\mathcal{D}}$
- Le terme $\Phi_2^j v_1 \equiv "la mère de v_1"$.
 $\Phi_2^j \mathcal{D} : \mathcal{D} \rightarrow \mathcal{D}$ telle que $\Phi_2^j \mathcal{D} ("Pierre") = "Marie"$.

Les structures de 1^{ier} ordre

③ Interprétation des formules non atomiques :

- La formule $F \equiv \Psi_n a \cdots z$ est interprétée par $F_{\mathcal{D}}$:
" $a_{\mathcal{D}}, \cdots, z_{\mathcal{D}}$ appartiennent à $\Psi_n \mathcal{D}$ ".
- La formule $F \wedge G$ est interprétée par " $F_{\mathcal{D}}$ et $G_{\mathcal{D}}$ ".
- La formule $\neg F$ est interprétée par "on n'a pas $F_{\mathcal{D}}$ ".
- La formule $\forall x F \langle x, y \rangle$ est interprétée par
"Quelque soit l'objet $c_{\mathcal{D}}$, on a $F_{\mathcal{D}} \langle c_{\mathcal{D}}, y_{\mathcal{D}} \rangle$ ".
- De cela découlent les autres interprétations :
 $F \vee G$ est interprétée par " $F_{\mathcal{D}}$ ou $G_{\mathcal{D}}$ "
 $F \Rightarrow G$ est interprétée par " $F_{\mathcal{D}}$ entraîne $G_{\mathcal{D}}$ ".

Les modèles de 1^{ier} ordre

④ Méta-Théorèmes :

- *Tous les domaines d'interprétation obtenus de cette façon sont des structures.*

En effet, l'interprétation est compatible avec le Modus Ponens et la règle de la généralisation.

- *Toutes les structures ainsi obtenues sont des modèles de la logique des prédicats du premier ordre.*

En effet, par construction de l'interprétation, toutes les tautologies seront interprétées comme des phrases vraies. De même, cette interprétation respecte les schémas de particularisation, de généralisation et de l'égalité.

Les modèles de 1^{ier} ordre

⑤ Méta-Théorèmes de cohérence et complétude :

- *La logique des prédicats du 1^{ier} ordre est cohérente.*

En effet, elle a des modèles où les formules F et non F s'interprètent par une phrase et sa négation, donc par une phrase vraie et une phrase fausse.

- (Méta-Théorème de complétude, Gödel, 1930)

Les théories des prédicats du premier ordre sont complètes pour l'ensemble des modèles des prédicats du premier ordre.

Si une formule est interprétée comme vraie dans tous les modèles de premier ordre, alors cette formule est un théorème. On peut démontrer toute formule pour laquelle il est impossible de trouver un contre-exemple.

Les logiques d'ordre supérieur

- Les logiques des prédicats du 2^{ième} ordre permettent de quantifier non seulement sur les variables (logique du 1^{ier} ordre) mais également sur des formules.

Ex. : $\forall F \text{ et } G, F \text{ et } G \text{ tautologies} \Rightarrow F \wedge G \text{ tautologie.}$

- (Premier théorème d'incomplétude, Gödel, 1930)

Si une théorie est assez puissante pour traduire l'arithmétique, elle est soit incohérente, soit incomplète.

Évidemment, cette théorie ne sera pas du premier ordre, ni du deuxième ordre, mais d'un ordre "infini", car l'arithmétique est capable de propositions **récurives**, c'est-à-dire de théorèmes parlant de théorèmes parlant de théorèmes parlant de ...

Les logiques d'ordre supérieur

- La théorie des prédicats $\mathcal{A}$ dont un modèle est l'arithmétique.
 - Une seule constante : 0
 - Un seul symbole fonctionnel à une place : $\sigma()$
 - Deux symboles fonctionnels à deux places : $+$ et $\times$
 - Un seul symbole prédicatif : $=$
 - Six axiomes spécifiques (en plus des axiomes de la théorie des prédicats) :

$$\sigma(x) = \sigma(y) \Rightarrow x = y \qquad x + 0 = x \qquad x \times 0 = 0$$

$$x + \sigma(y) = \sigma(x + y) \qquad \sigma(x) \neq 0 \qquad x \times \sigma(y) = x \times y + x$$

Les logiques d'ordre supérieur

- La théorie des prédicats $\mathcal{A}$ (suite).

- Un schéma d'axiome (récurrence) :

Si $F \langle x \rangle$ est une formule, alors

$$[F \langle 0 \rangle \wedge \forall x (F \langle x \rangle \Rightarrow F \langle \sigma(x) \rangle)] \Rightarrow \forall x F \langle x \rangle$$

est un axiome.

- Méta-théorème de Gödel sur la cohérence :

Si une théorie est assez puissante pour traduire l'arithmétique, comme l'est $\mathcal{A}$, il est impossible de prouver sa cohérence en utilisant seulement des procédés de démonstration formalisables dans cette théorie.

La théorie des ensembles

● Difficultés de définir les ensembles.

- Un ensemble est à la fois un objet et une collection d'objets.
- Les éléments d'un ensemble sont définis à partir de propriétés : Définition par extension ou par compréhension ?

● Paradoxe de Russel.

- *Soit E , l'ensemble des ensembles qui ont la propriété de n'être pas éléments d'eux-mêmes.*
- Alors l'ensemble x est élément de E si et seulement si l'ensemble x n'est pas élément de x .
- En appliquant cette propriété à l'ensemble E lui-même, on a :
- *L'ensemble E est élément de E si et seulement si l'ensemble E n'est pas élément de E .*

● *Tout théorie des ensembles essaie d'éviter ce paradoxe : Théorie des types ou de Zermelo-Fraenkel.*

La théorie de Zermelo-Fraenkel

- La théorie de Zermelo-Fraenkel.
 - La théorie Z.F. est une théorie des prédicats ayant un seul signe spécifique, $\in$.
 - $x \in y$ se lit comme *"le terme x appartient au terme y "* ou *"l'ensemble x appartient à l'ensemble y "*.
- L'interprétation de la théorie Z.F.
 - Soit $\mathcal{U}$, un ensemble intuitif, appelé **Univers**, muni d'une relation binaire $\in_{\mathcal{U}} : x \in_{\mathcal{U}} y$.
 - Attention : on parle ici d'ensemble intuitif, ce qui est différent des ensembles de la théorie Z.F.

Collections et Ensembles

- Définition d'un ensemble dans la théorie de Z.F.
 - On dit qu'une formule $F \langle x \rangle$ détermine un ensemble (composé des x qui la vérifient) lorsque :

$$\exists X \forall x (x \in X \iff F \langle x \rangle)$$

- Définition d'une collection stricte $\mathcal{A}$.
 - Si la formule F ne détermine pas un ensemble, on peut cependant lui faire correspondre la partie intuitive de $\mathcal{U}$ formée des objets a qui vérifient $F_{\mathcal{U}} \langle a \rangle$. On écrira : $x \tilde{\in} \mathcal{A}$ au lieu de $F \langle x \rangle$.

Exemples de collections strictes

- L'ensemble paradoxal de Russel.
- Autre exemple :
 - Soit $\mathcal{U}$ notre univers, composé d'ensembles d'entiers ayant un nombre impair d'éléments.
 - Si $F \langle x \rangle \Leftrightarrow x \leq 2$, alors $x = \{0, 1, 2\} \in \mathcal{U}$
 - Si $G \langle x \rangle \Leftrightarrow x \leq 3$, alors $x = \{0, 1, 2, 3\} \notin \mathcal{U}$.
D'où G ne définit pas un ensemble mais une collection.
 - Les parties intuitives de $\{0, 1, 2\} \in \mathcal{U}$ sont $\mathcal{P}_{\mathcal{U}}\{\{0, 1, 2\}\} = \{\emptyset, \{0\}, \{1\}, \{2\}, \{0, 1, 2\}\}$ mais pas $\{0, 1\}$.

Structure et modèle de la théorie de Z.

● Les axiomes

● Axiome 1 : L'axiome d'extentionnalité

Deux ensembles qui ont les mêmes éléments sont

égaux : $\forall x, y [\forall z (z \in x \Leftrightarrow z \in y) \Rightarrow x = y]$

Egalement, si deux objets sont égaux, ils possèdent les mêmes éléments.

● Axiome 2 : L'axiome de l'union

Etant donné un ensemble x , il existe un ensemble dont les éléments sont ceux des éléments de x :

$$\forall x \exists y \forall t [t \in y \Leftrightarrow \exists z (t \in z \wedge z \in x)]$$

Cet ensemble est unique, on peut le noter : $\bigcup_{z \in x} z$

Structure et modèle de la théorie de Z.

● Les axiomes (suite)

● Axiome 3 : L'axiome de l'ensemble des parties

Pour tout ensemble, il en existe un autre dont les éléments sont les parties du premier.

- On appelle **partie d'un ensemble** a , un ensemble b dont les éléments sont dans a : $\forall x (x \in b \Rightarrow x \in a)$
- Formule que nous noterons : $b \subseteq a$
- Cet ensemble est unique, on peut le noter : $\mathcal{P}x$

$$\forall x \exists y \forall t [t \in y \Leftrightarrow t \subseteq x] \text{ ou } \forall x \forall t [t \in \mathcal{P}_x \Leftrightarrow t \subseteq x]$$

(Voir la différence entre parties intuitives et parties de la théorie Z.F.)

Structure et modèle de la théorie de Z.

- Les axiomes (suite)

- Schéma 1 : Le schéma de substitution

L'image d'un ensemble par une relation fonctionnelle est un ensemble.

- On appelle **relation fonctionnelle** entre deux **ensembles** x et y , une relation telle que

$$\forall x ! y : \mathcal{R} \langle x, y \rangle$$

- $\mathcal{R}_{\mathcal{P}}(X)$ désigne **l'image d'un ensemble** X par la **relation** $\mathcal{R}$: $\mathcal{R}_{\mathcal{P}}(X) = \{y \mid \exists x(x \in X \wedge \mathcal{R} \langle x, y \rangle)\}$

- Donc, $(\forall x ! y \mathcal{R} \langle x, y \rangle) \Rightarrow \forall X \exists Y : Y = \mathcal{R}_{\mathcal{P}}(X)$

Structure et modèle de la théorie de Z.

- Théorie Z.F. = Théorie des Prédicats et les axiomes précédents

Attention, ceci suffit pour une théorie des ensembles, mais il n'y a pas d'ensemble infini dans cette théorie.

- Les premiers théorèmes

- Le schéma de compréhension

L'intersection d'une collection et d'un ensemble est un ensemble.

Démonstration : Il suffit de considérer la relation fonctionnelle " $\mathcal{R} \langle x, y \rangle \Leftrightarrow x = y \wedge y \tilde{\in} \mathcal{A}$ " et d'appliquer le schéma de substitution.

Structure et modèle de la théorie de Z.

● Les premiers théorèmes (suite)

● L'ensemble vide

*L'ensemble $\{x \in X \mid x \neq x\}$ est appelé **ensemble vide** et se désigne par $\emptyset$.*

- Il est unique par l'axiome d'extentionnalité.
- Comme $X \subseteq \emptyset \stackrel{def}{\Leftrightarrow} \forall x (x \in X \Rightarrow x \in \emptyset)$ et donc $X \subseteq \emptyset \Rightarrow X = \emptyset$, l'ensemble $\mathcal{P}\emptyset$ a un et un seul élément, $\emptyset$.
- Comme $X \subseteq \mathcal{P}\emptyset \stackrel{def}{\Leftrightarrow} \forall x (x \in X \Rightarrow x \in \mathcal{P}\emptyset)$ et donc $X \subseteq \mathcal{P}\emptyset \Leftrightarrow \forall x (x \in X \Rightarrow x = \emptyset)$, $\mathcal{P}\mathcal{P}\emptyset$ a exactement deux éléments, $\emptyset$ et $\mathcal{P}\emptyset$.

Structure et modèle de la théorie de Z.

- Les premiers théorèmes (suite)

- Le théorème de la paire

On peut construire un ensemble qui a pour seuls éléments deux ensembles donnés.

$$\forall x \forall y \exists z \forall t [t \in z \Leftrightarrow (t = x \vee t = y)]$$

- **Remarque :** Dans un premier jet de sa théorie, Zermelo n'avait pas pris pour schéma d'axiomes le schéma de substitution, mais celui de compréhension avec l'axiome de la paire. Fraenkel remarqua que c'était insuffisant pour une démonstration sur les ordinaux. Il les remplaça par le schéma de substitution. Depuis, on donne à la théorie le double nom de Zermelo-Fraenkel.

Structure et modèle de la théorie de Z.

● L'union et l'intersection

● L'union

On définit l'union de deux ensembles comme :

$$a \cup b \stackrel{def}{=} \cup \{x \mid x \in \{a, b\}\}$$

● L'intersection

On définit l'intersection de deux ensembles comme

$$a \cap b \stackrel{def}{=} \cap \{x \mid x \in \{a, b\}\}$$

● Autres définitions

- $a \setminus b \stackrel{def}{=} \{x \in a \mid x \notin b\}$

- $\{a, b, c\} \stackrel{def}{=} \{a, b\} \cup \{c\}$ et d'autres ensembles à quatre, cinq, ... éléments.

Modèle de la théorie de Z.F.

● Couples et produits cartésiens

● Couples

On définit le couple (a, b) comme $\{\{a\}, \{a, b\}\}$.

On a : $\forall a \forall b \forall c \forall d [(a, b) = (c, d) \Leftrightarrow a = c \wedge b = d]$.

● Produit cartésien et graphe

On définit **le produit cartésien** de deux ensembles A et B comme *l'ensemble*

$$A \times B = \{(a, b) \mid a \in A \wedge b \in B\} \subset \mathcal{PP}(A \cup B)$$

$$\text{car } (a, b) = \{a, \{a, b\}\} \in \mathcal{PP}(A \cup B)$$

Un graphe f est un *ensemble* de couples $\subset A \times B$.

$$\text{Dom}_f = \{x \mid \exists y (x, y) \in f\} \text{ et } \text{Im}_f = \{y \mid \exists x (x, y) \in f\}.$$

Modèle de la théorie de Z.F.

● Théorèmes de Cantor

● Il n'y a pas de surjection $\sigma : A \rightarrow \mathcal{P}A$

- Une surjection est un graphe $f \in A \times B$ tel que $\forall a \in A \exists ! b \in B$ tel que $(a, b) \in f$ (application = fonction partout définie) et $\forall b \exists a$ tel que $(a, b) \in f$.
- Démonstration : Si σ est une application, montrons qu'elle n'est pas surjective. Soit $B \stackrel{def}{=} \{x \in A \mid x \notin \sigma x\}$, nous allons voir que B ne peut pas être de la forme σa , avec $a \in A$. En effet, $x \in B \Leftrightarrow x \in A \wedge x \notin \sigma x$, et donc $x \in A \wedge x \in B \Leftrightarrow x \in A \wedge x \notin \sigma x$, ce qui serait absurde si l'on avait $B = \sigma a$. On aurait alors $x \in A \wedge x \in \sigma a \Leftrightarrow x \in A \wedge x \notin \sigma x$, ce qui est contradictoire pour $x = a$.
- Conclusion : il y a toujours plus d'éléments dans $\mathcal{P}A$ que dans A .

● L'ensemble des ensembles n'est pas un ensemble.

- Soit $\#(A)$ le nombre d'éléments de A . Le théorème de Cantor veut que $\#(A) < \#(\mathcal{P}(A))$. Mais si l'ensemble des ensembles est un ensemble (soit E), il contient donc l'ensemble de ses parties (qui est un ensemble par l'axiome des parties), et on aura $\#(\mathcal{P}(E)) < \#(E)$.

Biographie de Cantor



● CANTOR Georg Ferdinand, russe, 1845-1918

- “Cantor, d’origine danois, naquit à Saint-Pétersbourg. Il fit ses études en Allemagne où ses maîtres furent Weierstrass, Kummer et Kronecker. C’est dire qu’il s’intéressa à l’analyse et à la théorie des nombres, le noyau de ses recherches étant les difficultés rencontrées dans les concepts de limite et de continuité des fonctions et des courbes, indissociables de celui de nombre réel et d’un langage mathématique précis. Cantor professa à l’université de Halle dès 1879 et fut le fondateur de la Société des mathématiciens allemands (1890). Les conséquences de ses travaux allaient bouleverser les fondements des mathématiques, alors considérées comme inébranlables, jusqu’en 1963 avec les travaux de Gödel et de Cohen et la "découverte" de propositions indécidables (i.e. dont on ne peut prouver, au sein de la théorie elle-même et de par les axiomes qui la définissent, si elles sont vraies ou fausses).”

Serge Mehl,

<http://www.sciences-en-ligne.com/momo/chronomath/chrono1/Cantor.html>

Modèle d'Akermann

● Un modèle arithmétique pour la théorie des ensembles.

- On prend pour univers l'ensemble intuitif des entiers $\mathbb{N}$. Tout entier n peut s'exprimer en base deux et s'écrire d'une et une seule façon comme une somme de support fini :

$$n = \sum_{r \in \mathbb{N}} \epsilon_r^n 2^r \text{ où } \epsilon_r^n \in \{0, 1\}$$

- On définit $\in_{\mathbb{N}}$ par : $n \in_{\mathbb{N}} m \Leftrightarrow \epsilon_n^m = 1$.
- Par exemple : $\{1, 3, 4\} = 2^1 + 2^3 + 2^4 = 26$ et donc $1 \in_{\mathbb{N}} 26, 3 \in_{\mathbb{N}} 26$ et $4 \in_{\mathbb{N}} 26$.
- On a les axiomes d'extentionnalité (par l'unicité de la décomposition en base 2), de l'union (car l'union de partie finie donne un ensemble fini), de l'ensemble des parties (car le nombre de parties d'un ensemble fini est fini et détermine un entier), et le schéma de substitution .

Modèle d'Akermann

● Exemples.

- ① $0 = \emptyset$; $1 = \{0\}$ car $1 = 2^0$, d'où $1 = \{0\} = \{\emptyset\} = \mathcal{P}\emptyset$.
- ② $2 = \{1\}$ car $2 = 2^1$ mais $2 = \{1\} = \{\{0\}\} = \{\{\emptyset\}\}$
- ③ $3 = \{0, 1\}$ car $3 = 2^0 + 2^1$ d'où $3 = \{\emptyset, \{\emptyset\}\} = \mathcal{P}\mathcal{P}\emptyset$.
- ④ $\mathcal{P}6 = \mathcal{P}\{1, 2\} = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\} = \{0, 2, 4, 6\} = 2^0 + 2^2 + 2^4 + 2^6 = 84$.
- ⑤ Le graphe $f : \emptyset \rightarrow \emptyset$ a comme définition l'ensemble
$$f = \{(\emptyset, \emptyset)\} = \{\{\emptyset, \{\emptyset\}\}\} = \{\{0, \{0\}\}\} = \{\{0, 2^0\}\} = \{\{0, 1\}\} = \{2^0 + 2^1\} = \{3\} = 2^3 = 8$$
- ⑥ Le graphe f d'une bijection de 1 sur 2 est : $f : 1 = \{0\} \rightarrow 2 = \{1\} \Rightarrow f = \{(0, 1)\} = \{\{\{0\}, \{0, 1\}\}\} = \{\{1, 3\}\} = \{2^1 + 2^3\} = \{10\} = 2^{10} = 1024$.
- ⑦ Le plus petit graphe f d'une bijection entre deux ensembles distincts à deux éléments est 17 179 873 280. En effet, $17179873280 = 2^{12} + 2^{34} = \{12, 34\} = \{\{2, 3\}, \{1, 5\}\} = \{\{\{1\}, \{0, 1\}\}, \{\{0\}, \{0, 2\}\}\} = \{(1, 0), (0, 2)\}$
- ⑧ $f = \{(0, 0), (1, 2)\} = \{3, 68\} = 2^3 + 2^{68} = 295\,147\,905\,179\,352\,825\,864$
- ⑨ $f = \{(0, 1), (1, 2)\} = \{10, 68\} = 2^{10} + 2^{68} = 295\,147\,905\,179\,352\,826\,880$

BOOLE George, anglais, 1815-1864

● La logique de Boole :

● Si $A = \{x \mid F \langle x \rangle\}$ et $B = \{y \mid G \langle y \rangle\}$ alors

● $A \cap B = \{x \mid F \langle x \rangle \wedge G \langle x \rangle\}$

● $A \cup B = \{x \mid F \langle x \rangle \vee G \langle x \rangle\}$

● $A \setminus B = \{x \mid F \langle x \rangle \wedge \neg G \langle x \rangle\}$

● $A \subset B \Leftrightarrow \forall x F \langle x \rangle \Rightarrow G \langle x \rangle$

● $A \cap B = \emptyset \Leftrightarrow \forall x F \langle x \rangle \Rightarrow \neg G \langle x \rangle$

● A est l'univers si $F \langle x \rangle$ est une tautologie.



L'algèbre de Boole

● La structure de l'algèbre

- Un ensemble E possède une structure d'algèbre de Boole s'il est muni de deux lois de composition interne associatives et commutatives notées $+$ et $*$
- Les lois $+$ et $*$ sont distributives l'une par rapport à l'autre et admettent un élément neutre (0 et 1 respectivement)
- Tout élément de E est idempotent pour chaque loi : $x + x = x$ et $x * x = x$
- Tout élément x de E possède un unique élément, dit complémenté de x , généralement noté $\bar{x}$, vérifiant la loi du tiers exclu : $x + \bar{x} = 1$ et le principe de contradiction $x * \bar{x} = 0$. Dans cette algèbre, on peut écrire : $\bar{x} = 1 - x$.
- On a les propriétés dites de De Morgan: $\overline{x * y} = \bar{x} + \bar{y}$ et $\overline{x + y} = \bar{x} * \bar{y}$

● L'algèbre et la théorie des ensembles

- L'algèbre $(E, \cup, \cap)$ des parties d'un ensemble est une algèbre de Boole, la réunion ($\cup$) est l'addition ($+$) et l'intersection ($\cap$) est la multiplication ($*$). 1 est ici E et 0 est la partie vide et devient la partie complémentaire.
- Lois de Morgan : $\overline{A \cap B} = \bar{A} \cup \bar{B}$ et $\overline{A \cup B} = \bar{A} \cap \bar{B}$

La numérotation des éléments

● Les relations d'ordre.

- Une relation $\mathcal{R} <x, y>$ est appelée **relation d'ordre** si elle vérifie :

- $\forall x \forall y \forall z [(\mathcal{R} <x, y> \wedge \mathcal{R} <y, z> \Rightarrow \mathcal{R} <x, z>]$
(transitivité)

- $\forall x \forall y [(\mathcal{R} <x, y> \Rightarrow (\mathcal{R} <x, x> \wedge \mathcal{R} <y, y>)]$
(réflexivité)

- $\forall x \forall y [(\mathcal{R} <x, y> \wedge \mathcal{R} <y, x> \Rightarrow x = y]$
(antisymétrie)

- On la note $x \leq y$ et on pose $x < y \stackrel{def}{\Leftrightarrow} x \leq y \wedge x \neq y$
(ordre strict).

La numérotation des éléments

● Les collections ordonnées.

- Une collection $\mathcal{A}$ est ordonnée par $\mathcal{R}$ si $\mathcal{R}$ est une relation d'ordre sur les éléments de $\mathcal{A}$.
- L'ensemble A est un **ensemble ordonné** par $\mathcal{R}$ si $\mathcal{R} \subset A \times A$ et si $\mathcal{R}$ est une relation d'ordre.
- Soit $\mathcal{A}$ une collection ordonnée, on appelle **segment initial** une collection $\mathcal{B} \subset \mathcal{A}$ telle que $\forall x \forall y [(x < y \wedge x \in \mathcal{B}) \Rightarrow y \in \mathcal{B}]$.

On note le segment initial des éléments strictement inférieurs à l'élément a de $\mathcal{A}$: $\mathcal{S}_a \stackrel{def}{\Leftrightarrow} x \in \mathcal{A} \wedge x < a$.

La numérotation des éléments

- Les collections bien ordonnées.
 - Une relation est appelée **une relation de bon ordre** sur une collection $\mathcal{A}$ si pour tout élément $x \in \mathcal{A}$, S_x détermine un ensemble S_x , et que tout ensemble non vide contenu dans $\mathcal{A}$ possède un plus petit élément. Pour les ensembles bien ordonnés, seule la seconde condition subsiste.
 - **Principe de récurrence transfinie.** Si $\mathcal{A}$ est une collection bien ordonnée et si $\mathcal{C}\langle x \rangle$ est une collection telle que $\forall y \in \mathcal{A}[(\forall x < y, \mathcal{C}\langle x \rangle) \Rightarrow \mathcal{C}\langle y \rangle]$ alors $\forall x \in \mathcal{A}, \mathcal{C}\langle x \rangle$.

Les ordinaux

● La numérotation des éléments d'une collection

- Soit une collection $\mathcal{A}$ bien ordonnée et non vide. Elle a un plus petit élément a_0 . Considérons un élément quelconque a de $\mathcal{A}$. Soit c est le plus grand élément, soit il a un successeur, c'est-à-dire un plus petit majorant strict que nous noterons a^+ .
- On peut numérotter les éléments de $\mathcal{A}$ en partant du plus petit et en passant de chacun à son successeur. On généralise ainsi ce qu'on fait avec les entiers intuitifs.
- Question : Y a-t-il une seule façon de numérotter les éléments d'une collection ou d'un ensemble ?
- Réponse : Il n'y a qu'une seule manière de numérotter.

Les ordinaux

- Note : Les segments initiaux des entiers intuitifs sont $S_3 = \{0, 1, 2\}$, $S_4 = \{0, 1, 2, 3\}$, $\dots$ On a $S_4 = S_3 \cup \{3\}$.
- Numérotation de Robinson (USA, 1918-1974) : Les entiers n'ayant pas encore été définis ici, on posera :
 $0 \stackrel{\text{def}}{=} \emptyset$ $1 \stackrel{\text{def}}{=} 0 \cup \{0\} = \{0\}$ $2 \stackrel{\text{def}}{=} 1 \cup \{1\} = \{0, 1\}$
En général, $\alpha^+ = \alpha \cup \{\alpha\}$
- L'ensemble α est appelé un ordinal. Définition : α est un ordinal $\stackrel{\text{def}}{\iff} \alpha$ est transitif et $x \in y$ définit sur α une relation de bon ordre strict. [Un ensemble A est transitif $\stackrel{\text{def}}{\iff} \forall x(x \in A \Rightarrow x \subset A)$]. La collection des ordinaux est notée $\mathcal{O}_r$.



Les ordinaux

● Propriétés des ordinaux

- Si α est un ordinal, tous ses éléments sont des ordinaux.
- Deux ordinaux isomorphes sont égaux.
 - Rappel : Deux ensembles A et B sont isomorphes si et seulement si il existe une bijection f entre eux qui respecte l'ordre de chacun, c'est-à-dire $x < y$ dans $A \Rightarrow f(x) < f(y)$ dans B .
- La collection des ordinaux est une collection stricte.
 - Dém. : Si $\mathcal{O}_r$ est un ensemble, il est un ordinal lui-même car il est transitif et $x \in y$ est un bon ordre strict sur lui. Et donc, $\mathcal{O}_r \in \mathcal{O}_r$, ce qui est absurde car $\in$ doit définir un ordre strict sur $\mathcal{O}_r$.
- Il existe un isomorphe et un seul d'une collection bien ordonnée $\mathcal{A}$ sur un ordinal α ou sur $\mathcal{O}_r$.
 - Il n'y a qu'une seule façon de numérotter un ensemble ou une collection bien ordonnée.

Les ensembles et les ordinaux infinis

● Définition d'un ensemble infini

● Un ensemble E est infini : $\exists a \in E, \exists \sigma : E \mapsto E \setminus \{a\}$

● σ est une injection, c'est-à-dire : $x \neq y \Rightarrow \sigma(x) \neq \sigma(y)$

● Rien ne prouve l'existence d'ensembles infinis. Par exemple, le modèle d'Akermann ne possède pas d'ensemble infini.

● Axiome de l'infini.

● Il existe un ensemble infini.

● Nous appellerons théorie de Zermelo-Fraenkel (Z.F.), celle que nous avons développée jusqu'à présent (axiomes d'extentionnalité, de l'union, des parties, le schéma de substitution et l'axiome de l'infini).

● Axiome de fondation.

● Zermelo (1871-1953) et Fraenkel (1891-1965) ont d'autre part inclu l'axiome de fondation. L'axiome de fondation dit que :

$\forall x \neq \emptyset \exists y \in x : (y \cap x = \emptyset)$. Cet axiome interdit à un ensemble d'être élément de lui-même ($x = \{x, y\}$) (cfr. paradoxe de Russel ou de Cantor).

● Pour pouvoir développer les mathématiques, il faut ajouter l'axiome du choix.

L'axiome du choix

- L'axiome du choix, pose le problème de la notion "d'existence" mathématique et a fait couler beaucoup d'encre... Il est à l'origine de la déstabilisation de la science mathématique au début du 20 ième siècle, souvent appelée crise des fondements. Récemment encore, de nombreux mathématiciens le contestaient. On peut l'énoncer de plusieurs manières équivalentes, plus ou moins complexes.
- La plus simple est l'assertion équivalente de Russell : Le produit cartésien de toute classe d'ensembles non vides est non vide.
- De façon équivalente : Pour toute classe d'ensembles non vides et disjoints, en nombre fini ou non, il existe un algorithme (fonction de choix) permettant d'extraire un élément et un seul dans chaque ensemble afin de constituer un nouvel ensemble non vide.
- De façon équivalente : Principe du bon ordre de Zermelo : Tout ensemble peut être bien ordonné.
- En conclusion : on peut numéroter tous les éléments de tous les ensembles bien ordonnés (pas les collections).

Note : Comment peut-on numéroter les éléments de $\mathbb{R}$ ou de $[0, 1]$?



B. Russell, 1872-1970)



L'axiome du choix

- Cet axiome ne pose problème que dans le cas d'un nombre infini non dénombrable d'ensembles : choisir, c'est discerner un élément parmi d'autres. Dans le cas fini ou dénombrable, les éléments peuvent être rangés, comptés; on peut alors choisir. Mais dans le cas infini non dénombrable, comment choisir dans un ensemble continu ?
- Des mathématiciens, et non des moindres, comme Peano, Hadamard, Lebesgue, Baire et Borel refusèrent l'axiome du choix.
- En 1938, Gödel montre que si la théorie des ensembles est cohérente sans l'axiome du choix et sans l'hypothèse du continu, alors elle le demeure avec leurs adjonctions.
- En 1963, Paul J. Cohen montre l'indépendance de l'axiome du choix et de l'hypothèse du continu de Cantor que l'on croyait liés, en démontrant l'indécidabilité de l'hypothèse du continu. Il met ainsi fin à la querelle et permet de distinguer les résultats qui peuvent être démontrés avec ou sans l'axiome du choix.

Les classes cardinales

● Les classes cardinales

● Ensembles équipotents :

Deux ensembles sont équipotents s'il existe une bijection de l'un sur l'autre. La relation "*x est équipotent à y*" est une relation d'équivalence sur l'univers. Soit A un ensemble, la classe d'équivalence de A est appelée **classe cardinale de A** et notée $\bar{\bar{A}}$.

On a donc $B \tilde{\subset} \bar{\bar{A}} \Leftrightarrow \exists f : A \xrightarrow{+} B \Leftrightarrow \bar{\bar{A}} \cong \bar{\bar{B}}$

● Relation d'ordre entre classes cardinales :

La relation "*Il existe une injection de A dans B* " se note $\bar{\bar{A}} \tilde{\leq} \bar{\bar{B}}$. Nous posons aussi : $\bar{\bar{A}} \tilde{<} \bar{\bar{B}} \stackrel{def}{\Leftrightarrow} \bar{\bar{A}} \tilde{\leq} \bar{\bar{B}} \wedge \bar{\bar{A}} \not\tilde{=} \bar{\bar{B}}$

● Théorème de Bernstein :

$$\forall x \forall y (\bar{\bar{x}} \tilde{\leq} \bar{\bar{y}} \wedge \bar{\bar{y}} \tilde{\leq} \bar{\bar{x}} \Leftrightarrow \bar{\bar{x}} \cong \bar{\bar{y}})$$

● Opérations sur les classes cardinales :

$$\text{On pose : } \sum_{i \in I} \bar{\bar{A}}_i \stackrel{def}{\Leftrightarrow} \overline{\overline{\bigcup (\{i\} \times A_i)}} \quad \prod_{i \in I} \bar{\bar{A}}_i \stackrel{def}{\Leftrightarrow} \overline{\overline{\prod_i A_i}}$$

$$\text{D'où : } \bar{0} + \bar{\bar{A}} = \bar{\bar{A}} \quad \text{et} \quad \bar{1} \cdot \bar{\bar{A}} = \bar{\bar{A}}$$

Les Cardinaux et les entiers naturels

● Définition : Les Cardinaux

On appelle *cardinal* un ordinal α qui n'est équipotent à aucun ordinal strictement inférieur.

● Conséquences :

- Si A est un ensemble bien ordonnable, il est donc équipotent à un et un seul cardinal qui est noté $\#A$ et appelé *cardinal de A* . On a donc $\#A \in \bar{\bar{A}}$ et $\#A$ est le seul cardinal appartenant à $\bar{\bar{A}}$.
- Lorsque c'est possible, on transpose aux cardinaux les opérations sur les classes cardinales. Par exemple, si A et B sont bien ordonnables, on a $\#A + \#B \stackrel{def}{=} \#[(\{0\} \times A) \cup (\{1\} \times B)]$ et $\#A \times \#B \stackrel{def}{=} \#(A \times B)$.
- Les cardinaux sont rangés en deux classes : les *alephs* ou cardinaux infinis et les *cardinaux finis*. *Les cardinaux finis sont les entiers naturels*.
- On dit qu'un ensemble est *fini* s'il est équipotent à un cardinal fini. Remarquons qu'un ensemble non ordonnable peut fort bien n'être ni fini, ni infini.

Les Alephs et les différents infinis.

- Définitions : L'Aleph zéro et l'infini dénombrable.

La collection des Alephs est une sous-collection des Ordinaux et est donc ainsi bien ordonnée par la relation d'ordre "*appartenance*". Par un théorème précédent, il y a un isomorphisme unique : $\aleph : \mathcal{O}_r \rightarrow \mathcal{A}_l : \alpha \mapsto \aleph_\alpha$. On a $\aleph_0 \stackrel{def}{=} \omega \stackrel{def}{=} \# \mathbb{N}$.

- On appelle **ensembles dénombrables** les ensembles équipotents à

$\aleph_0$ c'est-à-dire tels que $\#A = \omega = \aleph_0$. Par exemple :

$$\aleph_0 = \omega = \# \mathbb{N} = \#(\mathbb{N} \times \mathbb{N}) = \# \mathbb{Q} = \#((\mathbb{N})^k).$$

$\mathbb{N}$ est le plus petit infini car il est isomorphe au premier ordinal infini.

- A partir du dénombrable, on reste dans le dénombrable, sauf si on prend les parties. En effet, $\#\mathcal{P}(A) = 2^{\#A}$ car un ensemble à n éléments possède 2^n parties. Pour le voir, il suffit de remarquer que définir un sous-ensemble de A , c'est dire pour chaque élément a_i de A s'il appartient ou pas à ce sous-ensemble. Un sous-ensemble B est donc équivalent au n-uplet $(\delta_1, \delta_2, \dots, \delta_n)$ où $\delta_i = 1$ si $a_i \in B$ et 0 sinon. Il y a autant de sous-ensembles B que de n-uplets possibles ($= 2^n$).

- Par le théorème de Cantor, on sait que : $2^\omega > \omega$.

Les Alephs et les différents infinis.

● Définition : L'Aleph un et l'hypothèse du continu.

- **Continuité de $\mathbb{R}$** : Cantor montra que l'ensemble des parties de $\mathbb{N}$ est équipotent à $\mathbb{R}$. Et donc, $\#\mathbb{R} = 2^{\aleph_0}$.
- **L'hypothèse du continu** : C'est dire qu'il n'existe pas d'infini entre $\aleph_0$ et $2^{\aleph_0}$. Alors, $\#\mathbb{R} = \aleph_1$ et en général, $\aleph_{k+1} = 2^{\aleph_k}$. Cette proposition est indécidable. L'accepter ou la refuser est compatible avec la théorie Z.F.

● Remarques :

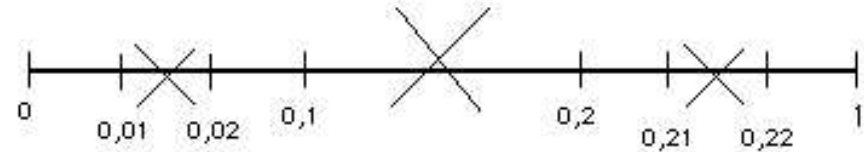
- Pour démontrer que $\#\mathbb{R} = 2^{\aleph_0}$, on montre que $\mathbb{R}$ est équipotent à n'importe quel intervalle continu, par exemple $[0, 1]$, puis on montre que tout réel de $[0, 1]$ peut s'inscrire comme une suite finie ou infinie de 0 et de 1. Il y a $2^{\aleph_0}$ possibles ω -uplets de 0 et de 1. On prend la décomposition en base $(\frac{1}{2})^n$: $0,75 = 0 \cdot (\frac{1}{2})^0 + 1 \cdot (\frac{1}{2})^1 + 1 \cdot (\frac{1}{2})^2 + 0 \cdots \simeq (0, 1, 1, 0, \cdots)$.
- Après 3 ans de travail pour prouver le contraire, Cantor a démontré l'équipotence entre le carré $[0, 1] \times [0, 1]$ et $[0, 1]$. Il écrivit à Dedekind : "*Je le vois, mais je ne le crois pas*". On a : $\aleph_1 = \aleph_1^2 = \aleph_1^k$.

La diagonale de Cantor.

- Comment prouver la non dénombrabilité de $\mathbb{R}$.
 - Soit l'intervalle $J =]0, 1[$. Tout ses éléments s'écrivent sous la forme $x = 0, x_1 x_2 \dots$ où les x_i sont les décimales de x .
 - Supposons que J soit dénombrable. On peut donc numéroté ses éléments avec les entiers de $\mathbb{N}$. Il existe donc une suite (u_n) de réels telle que $\forall x \in J : \exists n \mid x = u_n$
 - Mais les u_n peuvent aussi s'écrire sous la forme $u_n = 0, u_{n1} u_{n2} \dots$
 - Considérons un réel t défini ainsi : $t = 0, t_1 t_2 \dots$ où $t_i = 1$ si $u_{ii} \neq 1$ et $t_i = 2$ sinon.
 - Ce réel t ne peut être égal à aucun u_n de la suite car il sera toujours différent par la valeur de $t_i \neq u_{ii}$. Donc, la suite u_n n'épuise pas les réels de J .
 - Le réel t a été construit à partir des éléments diagonaux de la matrice des u_{ni} . Ce procédé est appelé *procédé de la diagonale de Cantor*.
 - Il permet de montrer la non dénombrabilité de *l'ensemble triadique de Cantor*. Cet ensemble est composé uniquement des réels de J ne s'écrivant qu'avec des 0 et des 2 comme décimales. Ici, $t_i = 0$ si $u_{ii} = 2$ et 2 si $u_{ii} = 0$.

L'ensemble triadique de Cantor.

● L'ensemble triadique de Cantor.

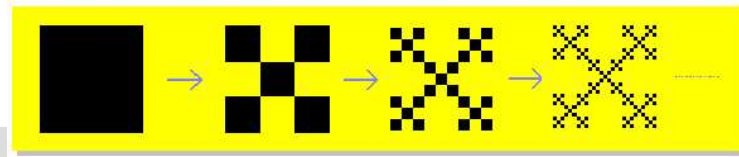


- Soit l'intervalle $J = [0, 1]$. Tous ses éléments sont écrits dans un système de numération en base 3 au lieu de 10.
- Au départ, on supprime au centre de l'intervalle le sous-intervalle $[0, 1; 0, 2[$. Il reste deux intervalles. Puis dans chaque intervalle restant, on supprime le sous-intervalle du milieu (ici, $[0, 01; 0, 02[$ et $[0, 21; 0, 22[$). Et ainsi de suite à l'infini. On obtient alors *les poussières de Cantor* ou *son ensemble triadique*.
- A la fin, on obtient un ensemble où tous les éléments de J ayant un "1" dans leur écriture en base 3 sont supprimés. En enlevant de l'intervalle J une infinité d'intervalles, et en ne gardant qu'une infinité de "points" détachés les uns des autres, Cantor pensait obtenir un ensemble dénombrable. Or le résultat J' a la puissance du continu (on le démontre par le procédé de la diagonale) et pourtant ne contient aucun sous-intervalle (en effet, tout sous-intervalle de longueur L sera "troué" à un moment par le procédé d'extraction). Sa longueur (de Lebesgue) est nulle (= somme des longueurs des sous-intervalles inclus dans J'). *La puissance du continu* n'est donc pas synonyme d'intervalle.

Le monde des fractals.

Les ensembles fractals.

- L'ensemble triadique de Cantor est un **ensemble fractal** de type auto-similaire. On peut faire la même chose avec un carré plein divisés en 9 sous-carrés, dont on enlève à chaque étape les 4 sous-carrés du milieu des bords.
- La dimension d d'un objet A peut être définie par l'équation suivante :
$$\mu(A/k) = \frac{\mu(A)}{k^d}$$
 où k est le rapport d'homothétie et $\mu(A)$ le volume (ou l'aire ou la longueur) de l'objet A . Par exemple, si on divise le rayon d'un cercle ou d'une sphère par $k = 2$, son volume ou son aire seront réduits par k^d . Et donc, $d = \frac{\log(\mu(A)/\mu(A/k))}{\log k}$.
- Soit n le nombre d'objets similaires qu'on obtient après l'homothétie. En géométrie classique, $n = \mu(A)/\mu(A/k)$. On définit **la dimension fractale ou de Hausdorff** d'un ensemble par : $d = \frac{\log(n)}{\log k}$, où n est le nombre d'objets similaires obtenus après le procédé fractal. Pour l'ensemble triadique, cela donne $d = \frac{\log 2}{\log 3} = 0,631$. La dimension du carré triadique est $d = \frac{\log 5}{\log 3} = 1,46$.

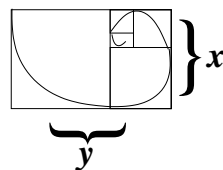


Les fractals et le nombre d'or.

- Les ensembles fractals ont la propriété d'être invariants par rapport aux homothéties : si l'on "zoom" sur un objet fractal, on retrouve le même objet avec la même structure.
- Pythagore** a conçu un rectangle fractal : il s'agit d'un rectangle tel que si on en supprime le carré inscrit, on retrouve un rectangle équivalent, et ainsi de suite. Il s'agit du **rectangle d'or** (associé à la spirale d'or), et le rapport de ses côtés $\frac{y}{x}$ est le **nombre d'or**. Le Parthénon d'Athènes a été construit sur un rectangle d'or.



Fibonacci
(1170-1250)



- Le nombre d'or $\Phi = \frac{y}{x} = \frac{1+\sqrt{5}}{2} = 1,618\dots$ est la solution de l'équation :
 $\frac{y}{x} = \frac{x}{y-x}$ ou $y^2 - x^2 - xy = 0$ ou $(\frac{y}{x})^2 - (\frac{y}{x}) - 1 = 0$
- Le nombre d'or apparaît aussi dans la suite de **Fibonacci** :
 $F(n) = F(n-1) + F(n-2)$ avec $F(1) = F(2) = 1$.
 La suite de Fibonacci : 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, ...
 Binet a prouvé : $F(n) = (\Phi^n - (\frac{-1}{\Phi})^n)/\sqrt{5} = [(\frac{1+\sqrt{5}}{2})^n - (\frac{1-\sqrt{5}}{2})^n]/\sqrt{5}$

Mandelbrot Benoît, Français, 1924.

- Polytechnicien, il s'installe aux Etats-Unis pour fuir le "terrorisme Bourbaki" et professe à l'université de Yale. Il est célèbre pour ses travaux concernant la géométrie *fractale* (substantif créé en 1975), qu'il étudia tout particulièrement chez IBM.
- Les irrégularités de la nature, d'apparence chaotique, sont en fait l'expression d'une géométrie très complexe de l'infiniment petit où la notion de dimension fractionnaire se substitue à celle de dimension euclidienne usuelle. Une courbe fractale est telle que toute portion est identique au tout. On retrouve les modèles fractals dans les nuages, les arbres, les fougères.



Gödel et l'incomplétude.



Kurt Gödel, 1906-1978)

- Référence : *Gödel : une révolution en mathématiques*, de André Delessert, Presses Polytechniques et Universitaires Romanes, 2000.
- Rappel : Deux questions restaient en suspens :
 - Le formalisme du premier ordre satisfait-il toutes les exigences des raisonnements mathématiques ?
Réponse positive en 1930 dans la thèse de doctorat de Gödel : "*Die Vollständigkeit der Axiome des logischen Kalküls*". C'est le *théorème de complétude de Gödel*.
 - Ce formalisme permet-il d'établir la non-contradiction des axiomes de l'arithmétique et de ceux des ensembles ?
Réponse négative en 1931 dans un article : "*Über formal unentscheidbare Sätze der Principia Mathematica und verwandte Systeme I*". Ce sont les *théorèmes d'incomplétude de Gödel*.

Les numéraux et les nombres naturels

- Nous avons défini les nombres entiers naturels. On sait que l'ensemble des nombres entiers forme un ensemble : ω , le premier ordinal limite. Il est facile dans le langage formel $L_{\mathbb{N}}$, qui est propre à l'arithmétique, d'en donner des échantillons précis : $0, 1, 1 + 1, (1 + 1) + 1, ((1 + 1) + 1) + 1, \dots$, etc. Le problème vient du "etc". En effet, il peut y avoir plusieurs langages formels $L_{\mathbb{N}}$ pour l'arithmétique et chacun donnera un sens différent au "etc".
- On appelle **numéral** tout nombre naturel qui peut être représenté graphiquement dans le langage formel $L_{\mathbb{N}}$. Plus précisément, un numéral doit pouvoir être écrit effectivement d'une manière au moins comme une formule de $L_{\mathbb{N}}$ ne comportant que les cinq signes " $(,), 0, 1, +$ ". Le numéral n'est pas essentiel à la démonstration de Gödel mais cela la simplifie. Les nombres naturels qui ne sont pas des numéraux sont des nombres si grands qu'aucune personne ou aucune machine ne pourra jamais les écrire.
- La notion de **numéral** permet de distinguer le monde idéal des mathématiques du monde concret des mathématiciens bien réels.

Le codage de Gödel.

- Considérons la liste (abrégée) des signes apparaissant dans les langages formels du premier ordre :

=	$\neg$	$\vee$	$\forall$	c	x	'	,	(	)
0	1	2	3	4	5	6	7	8	9

A tout agrégat A de signes du langage L_{IN} , en particulier pour toute formule, on peut attacher une suite de chiffres $\Sigma(A)$. Par exemple, $\Sigma((x = c)) = (8, 5, 0, 4, 9)$. A cette formule, on attache *le nombre de Gödel* $G((x = c)) = 2^8 \cdot 3^5 \cdot 5^0 \cdot 7^4 \cdot 11^9$

- On obtient un numéral qui est associé à toute formule ϕ de L_{IN} : $G(\phi)$. Ce numéral est unique et permet de retrouver la formule ϕ (il suffit de diviser par 2 autant de fois que c'est possible pour trouver le premier exposant, et donc le premier signe, puis de faire de même pour les autres nombres premiers).
- *La numérialisation de la logique du premier ordre élémentaire* est la donnée du nombre de Gödel pour toute suite finie (au sens fort) de formules de L_{IN} (c'est-à-dire des théorèmes). Si $\phi_1, \phi_2, \dots, \phi_n$ sont des formules de L_{IN} , alors $\Sigma(\phi_1, \phi_2, \dots, \phi_n) = (\Sigma(\phi_1), \Sigma(\phi_2), \dots, \Sigma(\phi_n))$.

Les récursives primitives de Gödel.

- Les fonctions numériques formelles (dites *récursives primitives*, appellation due à Kleene) sont au nombre de trois (à une ou plusieurs variables entières) :

- ① *la fonction successeur (incrémentation)* I définie par $I(n) = n + 1$
- ② *les fonctions constantes* $F_c(n_1, \dots, n_p) = c$ (entier) dont la fonction nulle notée simplement $N : N(n) = 0$
- ③ *les fonctions projections* $P_i(n_1, \dots, n_p) = n_i$. Par exemple, pour deux variables : $P_2(n_1, n_2) = n_2$; pour une variable : $P_1(n_1) = n_1$ est l'application identique.

- Deux règles de composition de fonctions récursives sont d'application :

- ① *Règle de composition* : Si $F(n_1, \dots, n_p)$ et $G_1, \dots, G_p$ sont des fonctions récursives primitives, alors $F(G_1, \dots, G_p)$ en est une.
- ② *Règle du principe de récurrence* : Si $F(0, n_2, \dots, n_p)$ et $G(n_0, n_1, \dots, n_p)$ sont des fonctions récursives primitives, et si $F(n + 1, n_2, \dots, n_p) = G(F(n, n_2, \dots, n_p), n, n_2, \dots, n_p)$ alors $F(n_1, n_2, \dots, n_p)$ est une fonction récursive primitive.

- Gödel a aussi défini des fonctions récursives générales mais elles ne sont pas nécessaires pour ses théorèmes.

Les récursives primitives de Gödel.

- Exemples de *fonctions récursives élémentaires* construites au moyen d'un nombre fini de règles. Notons que ces fonctions sont également des *fonctions numérales*.
- *La fonction prédécesseur D (décrémentation)* : si n est un entier, $n > 0 : D(n) = n - 1$. Elle sera définie par :
 - $D(0) = N(n)$ (i.e. = 0, condition d'arrêt)
 - $D(I(n)) = P_1(n)$ (récurrence)
- *La fonction addition $A : A(n, p) = n + p$* . Elle sera définie par :
 - $A(n, 0) = P_1(n)$ (i.e. = n , condition d'arrêt)
 - $A(n, p) = S(A(n, D(p)))$ (i.e. = $S(A(n, p - 1))$) : appel récursif
 - Par exemple : $A(2, 3) = S(A(2, 2)) = A(2, 2) + 1 = [S(A(2, 1)) + 1] + 1 = [[A(2, 0) + 1] + 1] + 1 = [[2 + 1] + 1] + 1 = [3 + 1] + 1 = 4 + 1 = 5$. On a fait ici 3 appels récursifs.
- *La fonction multiplication $M : M(n, p) = n \cdot p$* . Elle sera définie par :
 - $M(n, 0) = N(n)$ (i.e. = 0, condition d'arrêt)
 - $M(n, p) = A(M(n, D(p)), P_1(n, p))$ (i.e. = $n \cdot (p - 1) + n$) : appel récursif

L'arithmétisation de la logique.

- On peut montrer que si F est une fonction récursive primitive comportant p arguments, alors il existe dans $L_{\mathbb{N}}$ une formule $\phi(x_1, \dots, x_p, y)$ telle que l'égalité numérale $F(n_1, \dots, n_p) = m$ est vraie si et seulement si on peut prouver l'énoncé $\phi(n_1, \dots, n_p, m)$ dans $L_{\mathbb{N}}$.
- Autrement dit, tout calcul sur les numéraux effectués à l'aide des fonctions récursives primitives est l'interprétation d'un énoncé dérivable dans $L_{\mathbb{N}}$.
- Les fonctions récursives primitives permettent tous les calculs arithmétiques classiques. De plus, toutes les opérations logiques dans un système formel du premier ordre élémentaire peuvent être traduites par des calculs portant sur les nombres de Gödel des formules de $L_{\mathbb{N}}$, calculs réalisés par des fonctions récursives primitives. La vérification de ces faits est plus laborieuse que difficile. Elle conduit à une propriété importante :

Il existe une fonction récursive primitive F telle que les valeurs qu'elle prend sont exactement les nombres de Gödel des énoncés dérivables dans $L_{\mathbb{N}}$.

$\Rightarrow$ En regardant $Im(F)$, on a toutes les formules dérivables dans $L_{\mathbb{N}}$.

Le premier théorème d'incomplétude.

- ① Comme F est une fonction récursive primitive, elle-même est associée à une formule de $L_{\mathbb{N}}$, qui dit que **tel numéral (associé à une formule) appartient à $Im(F)$** . Par contradiction, il s'ensuit qu'il est possible d'exprimer par un énoncé $\alpha(n)$ dans $L_{\mathbb{N}}$ qu'un numéral donné n n'apparaît pas dans $Im(F)$.
- ② Numérotons toutes les formules de $L_{\mathbb{N}}$ à une variable libre x . Soit $\beta_n(x)$ la formule ayant n comme numéral.
- ③ D'où, $\alpha(n)$ signifie que la formule $\beta_n(x)$ n'est pas dérivable dans $L_{\mathbb{N}}$.
- ④ **Idée de Gödel** : $\alpha(x)$ est une formule à une variable libre de $L_{\mathbb{N}}$, et donc elle a également un numéral n_α , tel que $\alpha(x) \equiv \beta_{n_\alpha}(x)$.
- ⑤ **Paradoxe de Russel à la mode de Gödel** : Que signifie $\alpha(n_\alpha)$? Cela signifie que si $\alpha(n_\alpha)$ est dérivable dans $L_{\mathbb{N}}$, cela veut dire qu'il n'est pas dérivable. De façon inverse, si $\alpha(n_\alpha)$ n'est pas dérivable alors, par consistance de $L_{\mathbb{N}}$, cela signifie que $\neg\alpha(n_\alpha)$ est dérivable et donc $\beta_{n_\alpha}(n_\alpha)$ est faux, ce qui signifie que $\beta_{n_\alpha}(n_\alpha)$ - soit $\alpha(n_\alpha)$ - est dérivable dans $L_{\mathbb{N}}$. Contradiction.

Théorème : Si le système formel $L_{\mathbb{N}}$ pour l'arithmétique est consistant, alors il est incomplet. [car ni $\alpha(n_\alpha)$, ni $\neg\alpha(n_\alpha)$ ne sont dérivables dans $L_{\mathbb{N}}$.]

Le second théorème d'incomplétude.

Théorème : Si le système formel $L_{\mathbb{N}}$ pour l'arithmétique est consistant, alors $\text{Consis}(L_{\mathbb{N}})$ n'est pas dérivable dans $L_{\mathbb{N}}$.

- ① $\text{Consis}(L_{\mathbb{N}})$ signifie que l'énoncé $(0 = 1)$ n'est pas un théorème dans $L_{\mathbb{N}}$. Autrement dit, le nombre de Gödel de $(0 = 1)$ n'est pas dans $\text{Im}(F)$.
- ② Gödel démontre ce second théorème en montrant que si $\text{Consis}(L_{\mathbb{N}})$ était dérivable dans $L_{\mathbb{N}}$, alors $\alpha(n_{\alpha})$ serait aussi dérivable dans $L_{\mathbb{N}}$, ce qui est impossible d'après le premier théorème.
- ③ **Note 1** : Ce résultat a surpris les mathématiciens car il semble être auto-référentiel. En effet, il affirme que si $L_{\mathbb{N}}$ est consistant, alors on ne peut pas prouver que $L_{\mathbb{N}}$ soit consistant. Alors que la conclusion semble découler de l'hypothèse. De plus, si $L_{\mathbb{N}}$ n'est pas consistant, alors tout est démontrable, et donc $\text{Consis}(L_{\mathbb{N}})$ l'est aussi. Pourquoi ne pas affirmer que $\text{Consis}(L_{\mathbb{N}})$ est démontré dans tous les cas. Ceci est un raisonnement vicié, car c'est oublier ce que la consistance veut dire (que tout n'est pas démontrable). Un peu, comme lorsqu'un fou affirme que tout ce qu'il dit est vrai, cela ne veut pas dire que la phrase "je ne suis pas fou" est vraie.

Le second théorème d'incomplétude.

- ④ Note 2 : Les théorèmes de Gödel ne sont valides que dans les logiques de premier ordre de type fini (numéral). Gentzen, en 1943, a réussi à démontrer la consistance de $L_{\mathbb{N}}$ en utilisant des ordinaux dénombrables très grands, ce qui donne une preuve de longueur transfinie.
- ⑤ Note 3 : Tarski a démontré l'impossibilité de produire la formule $\alpha(x)$ du premier théorème de Gödel. Comme $\alpha(n)$ signifiait que la formule $\beta_n(x)$ ayant le nombre de Gödel n était dérivable dans $L_{\mathbb{N}}$, cela signifie qu'il n'existe pas de moyen mathématique ou informatique concret et fini de vérifier si une formule quelconque $\beta_n(x)$ est vraie ou non dans $L_{\mathbb{N}}$.
- ⑥ Note 4 : Les théorèmes de Gödel n'ont eu pas une grande influence sur les mathématiciens. L'image extérieure des mathématiques est celle d'une science solide, consistante, naturellement vraie. En effet, *"Le mathématicien a foi dans l'existence de modèles 'naturels', un pour l'arithmétique, un autre pour les nombres réels, un autre encore pour les ensembles et ainsi de suite. Cette attitude consiste à accepter des objets de pensée qui existent par eux-mêmes et non en vertu d'une preuve de non-contradiction. Elle ne prend de la logique mathématique que ce qui ne provoque aucun embarras."* (A. Delessert, *op cit*, page 217.)

Conclusions.

Que ce soit en logique, en théorie des ensembles, ou en arithmétique, la limite du raisonnement est toujours la production de **propositions auto-référentielles**, c'est-à-dire de propositions qui s'englobent elles-mêmes dans leur propre compréhension.

Le fait de pouvoir s'auto-comprendre, s'auto-intellectualiser, s'auto-identifier, s'auto-reconnaître n'est-ce pas également le propre de l'être humain, d'avoir conscience de soi. La limitation de la logique n'est-elle pas là ?